PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-288135
(43)Date of publication of application : 04.10.2002

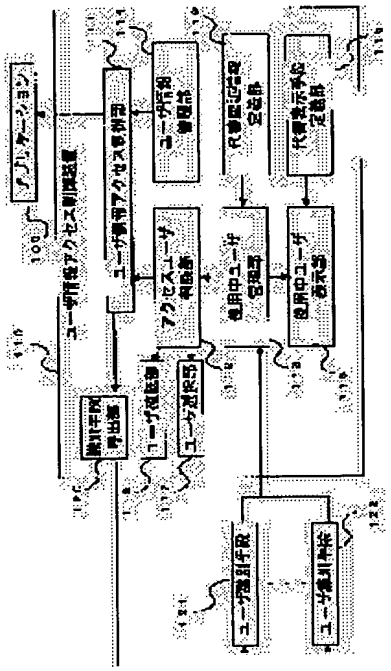
(51)Int.CI. G06F 15/00
G06F 12/00
G06F 12/14
H04L 9/32
H04N 7/173

(21)Application number : 2001-085464
(22)Date of filing : 23.03.2001

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : SAKUSHIMA HIROMI
MORIOKA MIKIO

(54) USER INFORMATION ACCESS CONTROLLING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a user information access controlling device that enables users to perform efficient access to user information, protecting the user information even if a plurality of users exist.
SOLUTION: The user information access controlling device 110 is provided with a plurality of user identifying means 121 and 122, an operating user controlling part 113 that controls information of a plurality of users understood as operating by the above identifying means, a user information access controlling part 111 that decides the user condition to define the requested status for terminal users when accessing to user information addressed by an application, an access user judging part 112 that obtains from the operating user controlling part the user conforming to the defined condition and the authentication level of the user, and a user information controlling part 114 that defines the authentication level condition to allow access to the user information. The super information access controlling device 10 is constituted so that it performs the access to the user information when the user conforms to the authentication level condition.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－288135
（P2002－288135A）
(43)公開日　平成14年10月４日(2002.10.4)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	15/00	３３０	Ｃ０６Ｆ	15/00	３３０Ｂ　５Ｂ０１７
	12/00	５３７		12/00	５３７Ａ　５Ｂ０８２
	12/14	３２０		12/14	３２０Ｃ　５Ｂ０８５
Ｈ０４Ｌ	9/32		Ｈ０４Ｎ	7/173	６４０Ａ　５Ｃ０６４
Ｈ０４Ｎ	7/173	６４０	Ｈ０４Ｌ	9/00	６７１　５Ｊ１０４

審査請求　未請求　請求項の数19　ＯＬ　（全９頁）

(21)出願番号　特願2001－85464(P2001－85464)

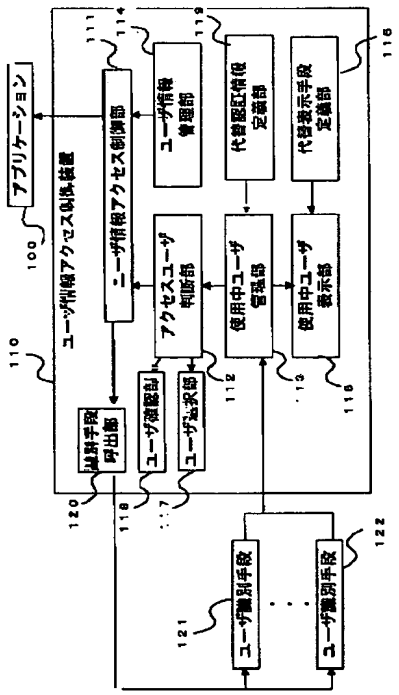
(22)出願日　平成13年３月23日(2001.3.23)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　佐久嶋　ひろみ
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　森岡　幹夫
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100099254
弁理士　役　昌明　（外３名）

最終頁に続く

(54)【発明の名称】　ユーザ情報アクセス制御装置

(57)【要約】　（修正有）
【課題】　利用者が複数に及ぶ場合でも、ユーザ情報の保護を図りながら、ユーザ情報への効率的なアクセスを可能にするユーザ情報アクセス制御装置を提供する。
【解決手段】　ユーザ情報アクセス制御装置110に、複数のユーザ識別手段121、122と、前記ユーザ識別手段により端末を使用中と判断された複数のユーザの情報を管理する使用中ユーザ管理部113と、アプリケーションの指定したユーザ情報にアクセスする際に、端末を使用するユーザのあるべき状態を規定するユーザ条件を決定するユーザ情報アクセス制御部111と、前記ユーザ条件を満たすユーザとユーザの認証レベルとを前記使用中ユーザ管理部より求めるアクセスユーザ判断部112と、ユーザ情報に対して、アクセスを許容する認証レベル条件を設定するユーザ情報管理部114とを設け、ユーザが認証レベル条件を満たすとき、アプリケーションの指定したユーザ情報へのアクセスを行うように構成している。



【特許請求の範囲】
【請求項１】　ユーザの使用状況に応じて、ユーザが使用する端末を制御する装置であって、
ユーザ識別手段と、
前記ユーザ識別手段により端末使用中と判断されたユーザの情報である使用ユーザ情報を管理する使用中ユーザ管理部と、
アプリケーションが指定するユーザ情報にアクセスする際に、端末を使用するユーザのあるべき状態を規定するユーザ条件を決定し、前記ユーザ条件を満たすとき、前記ユーザ情報へのアクセスを行うユーザ情報アクセス制御部と、
前記ユーザ条件を満たすユーザを前記使用中ユーザ管理部より求めて前記ユーザ情報アクセス制御部に伝えるアクセスユーザ判断部とを備えることを特徴とするユーザ情報アクセス制御装置。
【請求項２】　ユーザの使用状況に応じて、ユーザが使用する端末を制御する装置であって、
ユーザ識別手段と、
前記ユーザ識別手段により端末使用中と判断されたユーザの情報である使用ユーザ情報を管理する使用中ユーザ管理部と、
アプリケーションが指定するユーザ情報にアクセスする際に、端末を使用するユーザのあるべき状態を規定するユーザ条件と、認証レベルとを決定し、前記ユーザ条件を満たし、且つ、前記認識レベル条件を満たすとき、前記ユーザ情報へのアクセスを行うユーザ情報アクセス制御部と、
前記ユーザ条件を満たすユーザと当該ユーザの認証レベルとを前記使用中ユーザ管理部より求めて前記ユーザ情報アクセス制御部に伝えるアクセスユーザ判断部とを備えることを特徴とするユーザ情報アクセス制御装置。
【請求項３】　前記使用中ユーザ管理部の情報を視覚的に識別可能な代替情報に変換する代替表示手段定義部と、前記代替表示手段定義部が変換した代替情報を用いて前記使用中ユーザ管理部の情報を画面に表示する使用中ユーザ表示部とを備えることを特徴とする請求項１または２に記載のユーザ情報アクセス制御装置。
【請求項４】　前記使用中ユーザ管理部は、前記ユーザの識別時刻を管理し、前記アクセスユーザ判断部は、前記識別時刻の最も新しいユーザを前記ユーザ情報に該当するユーザとすることを特徴とする請求項１または２に記載のユーザ情報アクセス制御装置。
【請求項５】　前記使用中ユーザ管理部は、前記ユーザが現在使用中のデバイスの情報を管理し、前記アクセスユーザ判断部は、前記デバイスの情報が前記アプリケーションで指定された入力デバイス情報と一致するとき、前記デバイスを使用中のユーザを前記ユーザ情報に該当するユーザとすることを特徴とする請求項１または２に記載のユーザ情報アクセス制御装置。
【請求項６】　ユーザを選択するための選択画面を提示するユーザ選択部を備え、前記アクセスユーザ判断部は、操作者が前記選択画面で選択したユーザを前記ユーザ情報に該当するユーザとすることを特徴とする請求項１または２に記載のユーザ情報アクセス制御装置。
【請求項７】　該当するユーザに前記ユーザ情報へのアクセスの可不可を確認するユーザ確認部を備え、前記ユーザに、端末を使用する他のユーザが存在する状態での前記ユーザ情報へのアクセスの可不可を確認することを特徴とする請求項１または２に記載のユーザ情報アクセス制御装置。
【請求項８】　特定のユーザが端末を使用中であるときに、同時に使用中と見做されるユーザを定義する代替認証情報定義部を備えることを特徴とする請求項１または２に記載のユーザ情報アクセス制御装置。
【請求項９】　前記ユーザ識別手段を呼び出す識別手段呼出部を備え、前記アクセスユーザ判断部の指定するユーザ条件を満たすユーザが得られなかったとき、前記識別手段呼出部を通じて認証要求を行うことを特徴とする請求項２に記載のユーザ情報アクセス制御装置。
【請求項１０】　ユーザの使用状況に応じて、ユーザが使用する端末を制御するプログラムであって、
コンピュータに、
端末を使用しているユーザを識別する手順と、
端末を使用しているユーザの情報である使用ユーザ情報を管理する手順と、
アプリケーションが指定するユーザ情報にアクセスする際に、端末を使用するユーザのあるべき状態を規定するユーザ条件を決定する手順と、
前記使用ユーザ情報が前記ユーザ条件を満たしているか否かを判断する手順と、
前記使用ユーザ情報が前記ユーザ条件を満たしている場合に、ユーザ情報へアクセスする手順とを実行させるためのプログラム。
【請求項１１】　ユーザの使用状況に応じて、ユーザが使用する端末を制御するプログラムであって、
コンピュータに、
端末を使用しているユーザを識別する手順と、
端末を使用しているユーザの情報である使用ユーザ情報を管理する手順と、
アプリケーションが指定するユーザ情報にアクセスする際に、端末を使用するユーザのあるべき状態を規定するユーザ条件と、認証レベルとを決定する手順と、
前記使用ユーザ情報が前記ユーザ条件及び認証レベルを満たしているか否かを判断する手順と、
前記使用ユーザ情報が前記ユーザ条件及び認証レベルを満たしている場合に、ユーザ情報へアクセスする手順とを実行させるためのプログラム。
【請求項１２】　前記コンピュータに、さらに、
前記使用ユーザ情報を視覚的に識別可能な代替情報に変

換する手順と、
前記代替情報を用いて前記使用ユーザ情報を画面に表示する手順とを実行させるための請求項１０または１１に記載のプログラム。
【請求項１３】　前記コンピュータに、さらに、
前記使用ユーザ情報に、前記ユーザの識別時刻を含めて管理する手順と、アクセスするユーザ情報の対象のユーザとして前記識別時刻の最も新しいユーザを選定する手順とを実行させるための請求項１０または１１に記載のプログラム。
【請求項１４】　前記コンピュータに、さらに、
前記使用ユーザ情報に、ユーザが現在使用中のデバイスの情報を含めて管理する手順と、前記デバイスの情報がアプリケーションで指定された入力デバイス情報と一致するとき、アクセスするユーザ情報の対象のユーザとして、前記デバイスを使用中のユーザを選定する手順とを実行させるための請求項１０または１１に記載のプログラム。
【請求項１５】　前記コンピュータに、さらに、
ユーザを選択するための選択画面を提示する手順と、前記選択画面でユーザが選択操作を行ったとき、アクセスするユーザ情報の対象のユーザとして、前記操作を行ったユーザを選定する手順とを実行させるための請求項１０または１１に記載のプログラム。
【請求項１６】　前記コンピュータに、さらに、
ユーザに対して、端末を使用する他のユーザが存在する状態での前記ユーザ情報へのアクセスの可不可を確認する手順を実行させるための請求項１０または１１に記載のプログラム。
【請求項１７】　前記コンピュータに、さらに、
特定のユーザが端末を使用中であるときに、同時に使用中と見做されるユーザを定義する手順を実行させるための請求項１０または１１に記載のプログラム。
【請求項１８】　前記コンピュータに、さらに、
前記使用ユーザ情報が前記ユーザ条件を満たすが前記認証レベルを満たしていないとき、ユーザに対して認証要求を行う手順を実行させるための請求項１０または１１に記載のプログラム。
【請求項１９】　ユーザの使用状況に応じて、ユーザが使用する端末を制御するプログラムであって、
コンピュータに、請求項１から９のいずれかに記載の機能を実現させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、複数のユーザが同時に利用するデジタルテレビなどの端末において、ユーザ情報へのアクセスを制御するユーザ情報アクセス制御装置に関し、特に、ユーザ情報の保護を図りながらユーザ情報へのアクセスを可能にするものである。
【０００２】
【従来の技術】従来のパーソナルコンピュータは、ユーザが単独で使用することを前提に構成されており、この場合、ログイン時の認証などにより、ユーザには自己のユーザ情報へのアクセス権が与えられる。別のユーザのユーザ情報にアクセスするためには、一度ログアウトし、あるいは新たな認証を経て、アクセスのためのユーザ権限を得るなどの手順が必要になる。
【０００３】また、サーバが管理するユーザ情報をネットワーク接続された複数の端末から同時にアクセスする技術は従来から知られている。この場合、情報を要求するユーザは、それぞれの端末において必要な認証を行うだけでユーザ情報に対するアクセスが許可される。ただ、これは、複数のユーザが同じ画面を同時に見るという状態ではない。
【０００４】一方、デジタルテレビの端末では、複数のユーザが同時に画面を見ると云う状況が発生する。この端末は、近い将来、ユーザの視聴履歴を蓄積し、それを基にユーザの嗜好に沿った番組情報を選択して提示することが可能になり、また、放送系以外に、インターネットを通じて取得した情報を表示したり、電子ショッピングや電子メールの交換などを行うことなどが可能になる。
【０００５】こうした機能を備える端末は、多種類のユーザ情報を扱うことになる。例えば、ユーザごとの視聴履歴や、各人のお気に入りサイトを表すブックマーク、電子決済に使用するクレジットカードの番号、個人宛のメールなどである。これらのユーザ情報は、ユーザがそれを入力したり、その利用や確認のために呼び出したりする場面で、画面に表示されることになる。
【０００６】こうしたユーザ情報の保護を図るため、従来は、その個人データの秘匿性に応じた認証レベルを設定し、認証レベルを満たすユーザのみがその情報に接することができるように制限を設けている。
【０００７】
【発明が解決しようとする課題】しかし、デジタルテレビなど、同時に複数のユーザが利用する端末では、アプリケーションの処理のためにユーザ情報へのアクセスが必要となる場合に、ユーザを特定するところから始めなければならないが、これまで、複数の人が同時に端末を利用する環境の下で、アクセスするユーザ情報の秘匿性などに応じて、ユーザの特定を効率的に行う方式については、未だ開発が進められていない。
【０００８】また、複数のユーザが同時に閲覧する端末に対して、ユーザの認証レベルに応じた個人情報の表示が許容される方式を単純に適用すると、表示されたユーザの個人情報が、同時に利用している他のユーザにも知られてしまうと云う不都合が生じる。
【０００９】本発明は、こうした従来の問題点を解決するものであり、利用者が複数に及ぶ場合でも、ユーザ情報の保護を図りながら、ユーザ情報への効率的なアクセ

スを可能にするユーザ情報アクセス制御装置を提供することを目的としている。

【００１０】

【課題を解決するための手段】そこで、本発明では、ユーザ情報アクセス制御装置に、ユーザ識別手段と、ユーザ識別手段により端末使用中と判断されたユーザの情報（使用ユーザ情報）を管理する使用中ユーザ管理部と、アプリケーションが指定するユーザ情報にアクセスする際に、端末を使用するユーザのあるべき状態を規定するユーザ条件を決定し、前記ユーザ条件を満たすとき、前記ユーザ情報へのアクセスを行うユーザ情報アクセス制御部と、前記ユーザ条件を満たすユーザを使用中ユーザ管理部より求めてユーザ情報アクセス制御部に伝えるアクセスユーザ判断部とを設けている。

【００１１】また、ユーザ情報アクセス制御装置に、ユーザ識別手段と、ユーザ識別手段により端末使用中と判断されたユーザの使用ユーザ情報を管理する使用中ユーザ管理部と、アプリケーションが指定するユーザ情報にアクセスする際に、端末を使用するユーザのあるべき状態を規定するユーザ条件と、認証レベルとを決定し、前記ユーザ条件を満たし、且つ、前記認識レベル条件を満たすとき、前記ユーザ情報へのアクセスを行うユーザ情報アクセス制御部と、前記ユーザ条件を満たすユーザと当該ユーザの認証レベルとを使用中ユーザ管理部より求めてユーザ情報アクセス制御部に伝えるアクセスユーザ判断部とを設けている。

【００１２】そのため、端末を使用するユーザが複数に及ぶ場合でも、ユーザ条件を満たすときだけユーザ情報へのアクセスが行われ、ユーザ情報の保護を図りながら、ユーザ情報へのアクセスの効率化を図ることができる。

【００１３】なお、この明細書で本発明を説明するために使用する「認証レベル」と云う用語は、データに対するアクセス権限やプログラムに対する実行権限を認証するためのレベルの意味で使用する。

【００１４】

【発明の実施の形態】本発明の実施形態におけるユーザ情報アクセス制御装置は、図１に示すように、ユーザ情報を管理するユーザ情報管理部114と、任意のアプリケーション100からユーザ情報へのアクセスが要求された場合に、ユーザ情報管理部114に管理されたユーザ情報へのアクセスを制御するユーザ情報アクセス制御部111と、使用中のユーザを識別するユーザ識別手段121、122の情報に基づいて使用中のユーザとその認証レベルとを管理する使用中ユーザ管理部113と、代替認証を定義する代替認証情報定義部119と、使用中のユーザを視覚的に識別可能な代替情報に変換する代替表示手段定義部115と、必要に応じて使用中のユーザを代替情報により表示するための表示処理を行う使用中ユーザ表示部116と、使用中のユーザの中からユーザ情報の対象となるユーザとその認証レベルとをユーザ情報アクセス制御部111に伝えるアクセスユーザ判断部112と、必要に応じてユーザ情報の該当者を選択するためのユーザ選択部117と、必要に応じてユーザ情報の該当者にユーザ情報の表示の是非を確認するユーザ確認部118と、所定の認証レベルを求める必要がある場合にユーザ識別手段121を呼び出すための識別手段呼出部120とを備えている。

【００１５】なお、このユーザ情報管理部114、ユーザ情報アクセス制御部111、使用中ユーザ管理部113、代替認証情報定義部119、代替表示手段定義部115、使用中ユーザ表示部116、アクセスユーザ判断部112、ユーザ選択部117、ユーザ確認部118、及び識別手段呼出部120の各々は、コンピュータがプログラムに従って動作することにより実現される。

【００１６】ユーザ識別手段121、122は、特別なデバイスを必要としないユーザＩＤとパスワードとでユーザを認証する認証手段の他、ＩＣカード、指紋、声紋、虹彩などを用いた認証手段、さらには決められたリモコンボタンや画面上のアイコンの選択のみでユーザを識別する手段を含む。

【００１７】ユーザ情報アクセス制御装置110の使用中ユーザ管理部113は、ユーザ識別手段121、122の情報に基づいて、図４に示すように、ユーザのユーザＩＤ、ユーザが用いたユーザ識別手段121、122により決まる認証レベル（例えばリモコンボタンのボタンを押すのみの認証レベルは低いが、ＩＣカードを使った場合の認証レベルは高くなる。なお、この明細書では、認証レベルの数値が小さい程、認証レベルは高いものとして説明する）、識別時刻、及び、使用している入力デバイスＩＤ等の情報を含むユーザ管理情報を生成し、現在使用中のユーザを管理する。

【００１８】また、ユーザ情報管理部114で管理されているユーザ情報は、図２に示すように、階層構造を取り、それぞれのノードとなるユーザ情報（図２における201、211、221、231、241）には、読み込み、書き込みそれぞれに対する認証レベル条件及びデータアクセスタイプが設定されている。

【００１９】データアクセスタイプは、図３に示すように、ユーザ情報にアクセスするためのユーザ条件（使用中のユーザ数やユーザタイプ、ユーザの特定方法などに関する条件）と対応付けて規定されている。例えば、データアクセスタイプがSINGLE_W（Wは書込時のデータアクセスタイプであることを示している）の場合は、使用中のユーザが一人である必要があり、MULTI_R（Rは読込時のデータアクセスタイプであることを示している）の場合は、使用中のユーザが複数であっても許容される。また、USER_TYPEの場合は、使用中のユーザの全てが大人である、と云うように、使用者のユーザタイプが全て同じであることを必要とする。また、ANY_ONEの場合は、使用中のユーザが複数のときに、誰か一人を適宜

選ぶ必要があり、SELECT_ONEの場合は、使用中のユーザが複数のときに、特定の一人を厳密に選ぶ必要がある。

【００２０】ユーザ情報アクセス制御部111は、この図３のテーブルを保持しており、端末のアプリケーション100からユーザ情報へのアクセス要求があったとき、そのユーザ情報のデータアクセスタイプから求めたユーザ条件が満足され、且つ、ユーザ情報に対する認証レベルが満足されるとき、そのユーザ情報へのアクセスを実行する。

【００２１】図７は、このときの基本手順を示している。

ステップ１：アプリケーション100は、ユーザ情報アクセス制御装置110のユーザ情報アクセス制御部111にユーザ情報へのアクセスを要求する。

ステップ２：ユーザ情報アクセス制御部111は、ユーザ情報管理部114に管理された該当するユーザ情報からデータアクセスタイプを取得し、

ステップ３：データアクセスタイプからユーザ条件を決定し、これをアクセスユーザ判断部112に伝える。

【００２２】ステップ４：アクセスユーザ判断部112は、使用中ユーザ管理部113から使用中のユーザとその認証レベルとを求め、

ステップ５：ユーザ条件を満たしているか否かを判断する。ユーザ条件を満たしているときは、

ステップ６：使用中のユーザのユーザＩＤと認証レベルとをユーザ情報アクセス制御部111に伝える。これを受けて、ユーザ情報アクセス制御部111は、その認証レベルが、ユーザ情報管理部114に管理された該当するユーザ情報の認証レベルを満足するかどうかを識別し、満足するときは、

ステップ７：ユーザ情報へのアクセスを実行する。

【００２３】また、ステップ５においてユーザ条件を満足しないとき、及び、ステップ６において認証レベルを満足しないときは、ユーザ情報へのアクセスを拒絶する。

【００２４】具体的な例として、ユーザがコンテンツの閲覧操作を行った場合について説明する。アプリケーションであるブラウザは、ユーザ情報アクセス制御部111に対し、現在使用中のユーザ全ての履歴データに、閲覧情報を書き込むことを要求する。この履歴データは、ユーザ情報管理部114で管理されており、そのデータアクセスタイプがMULTI_Wであるとする。この場合のユーザ条件は、図３から「１人以上」となる。そこで、ユーザ情報アクセス制御部111は、アクセスユーザ判断部112に対し、ユーザ条件を１人以上として要求する。

【００２５】図４の例では、使用中ユーザ管理部113が管理している使用中ユーザは３人であり、ユーザ条件を満たしている。そこで、アクセスユーザ判断部112は、この３人のユーザのユーザＩＤと認証レベルとをユーザ情報アクセス制御部111へ返す。ユーザ情報アクセス制御部111は、返された各ユーザの認証レベルを、ユーザ情報管理部114より求めた履歴データに対する書き込み認証レベル条件と照合し、この認証レベル条件を満たす全てのユーザの履歴データに閲覧情報が書き込まれるように制御する。

【００２６】また、使用中ユーザ表示部116は、使用中ユーザ管理部113が管理しているユーザ管理情報に基づいて、画面に使用中ユーザを示すアイコンを表示する。また、画面には、ユーザ識別情報の他に、ユーザの認証レベルや使用中の入力デバイス情報を同時に表示してもよく、これらの情報は、形、色、濃淡、大きさ、点滅と云う代替情報に置き換えて表示してもよい。使用中ユーザ管理部113より得られる情報をどのような視覚情報に置き換えるかの定義は代替表示手段定義部115で行われる。

【００２７】このように、使用中のユーザを表示することにより、現在の使用中ユーザの状態をユーザ自身が常に認識することができ、自分の履歴データが更新されていることを把握することができる。また、端末を使用（閲覧）しているのに、自己のアイコンが表示されていない場合には、ユーザ情報アクセス制御装置110が自分を正常に認識していないことをユーザは知ることができる。この場合、ユーザはリモコンボタンを押す等の操作でユーザ情報アクセス制御装置110の認識を正常化することができる。これにより、ユーザが認識しないうちに不要なデータが書き込まれたり、また、必要なデータを保存し損なったりすることを防ぐことができる。

【００２８】また、ＥＣ（電子商取引）手続き処理などの中で、ユーザが予め入力したクレジットカード番号を、ユーザに確認を求めるために表示する場面を考える。このクレジットカード番号の読み込みに対するデータアクセスタイプは、図２に示すように、USER_TYPEと設定されているものとする。そのため、このデータアクセスタイプから、図３により、同じユーザタイプのユーザのみが使用中であるときは、アクセス可能と判断される。

【００２９】この場合、アクセスユーザ判断部112は、使用中ユーザ管理部113から使用中ユーザのユーザＩＤを取得し、ユーザ情報管理部114に管理されているユーザ情報から、各ユーザＩＤのユーザタイプを調べる。そして、使用中のユーザが全て同じユーザタイプであるとき、そのユーザＩＤと認証レベルとをユーザ情報アクセス制御部111へ伝える。ユーザ情報アクセス制御部111は、その認証レベルがクレジットカード番号の読み込み時の認証レベル条件を満たす場合にのみ、クレジットカード番号を表示する。こうすることにより、例えば、家族のうち大人はクレジットカード番号を見てもよいが、子供が見ることは避けるといったことが可能となる。

【００３０】次に、メールを例に取る。受信したメールはユーザ情報管理部114で管理され、メール通知情報を

参照するためのデータアクセスタイプはMULTI_Rとする。ユーザ情報アクセス制御部111は、アプリケーション100からメール通知情報へのアクセス要求が有ったとき、ユーザ条件を１人以上としてアクセスユーザ判断部112に伝え、アクセスユーザ判断部112から使用中のユーザ全てについてのユーザＩＤと認証レベルとを得る。その結果、認証レベル条件を満たす全てのユーザのメールボックスが読み込まれ、端末を複数人が同時に使用している場合でも、端末にメール着信状態が表示される。

【００３１】一方、メールの内容を参照するためのデータアクセスタイプは、SINGLE_Rとする。メールアプリケーションが特定のユーザのメール表示を要求した場合、ユーザ情報アクセス制御部111は、アクセスユーザ判断部112にユーザ条件を１人と指定する。このとき、アクセスユーザ判断部112が使用中のユーザを一人と判断できなければ、アクセス拒否となる。

【００３２】この場合、ユーザ確認部118は、アクセスユーザ判断部112の判断結果を受けて、アクセス拒否となった理由を、例えば「メールを表示すると他の人にも見られてしまいます。それでもいいですか？」と云うようなメッセージで表示する。ユーザがメール表示の許可操作を行えば、アクセスユーザ判断部112は、その１人のユーザＩＤと認証レベルとをユーザ情報アクセス制御部111へ伝え、そのメールの表示が実行される。一方、ユーザがメール表示に対し拒否操作を行えば、メールは表示されない。

【００３３】このように、現在のユーザ状況はユーザ情報の安全性を脅かす虞れがあることをユーザに知らせ、ユーザがそれを確認した上でユーザ情報へのアクセスを指示した場合に、そのユーザ情報へのアクセスが行われる。こうすることにより、安全性を確保しながらスムーズに情報へアクセスすることが可能となる。

【００３４】また、この例のように、複数のユーザのうちの一人だけのユーザ情報にアクセスするために、ユーザの特定が必要になる場合がある。このとき、アプリケーションにより操作デバイスが明確である場合は、入力デバイス情報からユーザを特定することができる。しかし、各ユーザが操作中であるような場合には、ユーザの特定が難しい。

【００３５】この場合でも、そのユーザ情報のデータアクセスタイプがSELECT_ONEであるときは、ユーザを厳密に特定する必要がある。アクセスユーザ判断部112は、ユーザ情報アクセス制御部111から、SELECT_ONEのユーザ条件である「複数人中ユーザ特定」の指定を受けると、ユーザ選択部117を通じて、図５に示すように、ユーザ選択画面に使用中ユーザ管理部113で管理されているユーザを、名前やアイコンなどで表示する。操作者がこの画面からユーザを選択すると、アクセスユーザ判断部112は、選択されたユーザのユーザＩＤと認証レベルとをアクセスユーザ判断部112に返す。このように、ユーザ選択部117を持つことにより、ユーザを厳密に特定することが可能になる。

【００３６】これにより、複数人が同時に端末を利用し、ユーザを自動的に判断することが難しい場合でも、簡単な操作でアクセスユーザを選択することができるようになる。

【００３７】また、ユーザ情報が、重要性を持たない例えばゲームの得点記録等であって、データアクセスタイプがANY_ONEであるときは、ユーザ情報アクセス制御部111は、アクセスユーザ判断部112に対して、そのユーザ条件である「複数人中一人自動選択」を指定する。これを受けたアクセスユーザ判断部112は、使用中ユーザ管理部113が管理する使用中ユーザの中で識別時刻が最も新しいユーザのユーザＩＤと認証レベルとをユーザ情報アクセス制御部111に返す。また、このとき、使用中ユーザ表示部116に表示した該当するユーザのアイコンを点滅表示して、選択した者が誰であるかを知らせる。識別時刻は、リモコンのユーザ識別ボタンを押して切り替えることが可能であり、この操作でユーザ情報を表示するユーザを簡単に更新することができる。

【００３８】このように、複数人が同時に端末を利用する状況の下で、取り敢えず誰かのユーザ情報を読み出す必要があるときでも、簡便にユーザを指定することができ、また、そのユーザを簡便に更新することができる。また、順次操作ユーザが変わりながらユーザデータにアクセスするような場合でも、簡単な操作でアクセスユーザを変えることができる。

【００３９】また、幼児や老人など、あまりリモコン等の操作は行わないが閲覧は行うユーザに対しては、代替認証情報定義部119で、父親や母親が使用者である時、同時に幼児や老人も使用者であると定義することができる。図６は、代替認証情報定義部119での定義を示している。この定義に基づいて、ユーザＩＤ１である主たる操作者が認証レベル２より低い認証レベル（認証レベルの数値は２以上となる）で使用しているとき、同時に、ユーザＩＤ２及び３のユーザが、認証レベル３の状態で使用しているものと識別される。

【００４０】これにより、父親や母親が操作している時でも、同時に子供の情報にアクセスことが可能になり、例えば、子供宛のメール着信通知を表示することもできる。即ち、代替認証を行うことにより、通常、端末操作を行わないユーザに対するユーザ情報にもアクセスすることが可能になる。

【００４１】また、ユーザ情報へのアクセス可否の判断において、ユーザ条件は満たしているが、認証レベル条件を満たしていない場合、ユーザ情報アクセス制御部111は、使用中のユーザを識別手段呼出部120で呼び出し、ユーザ情報で規定された認証レベルでの認証を求めることができる。使用中のユーザは、リモコンでの認証レベルから、求めに応じて、例えばＩＣカードを用いた認証

を実行する。その結果、認証レベル条件が満足され、ユーザ情報へのアクセスが実行される。

【００４２】これにより、任意の操作でユーザ情報にアクセスしようとした場合に、該当する認証レベルのユーザが存在しないときでも、その場で必要なユーザ認証を行うことにより、ユーザ情報へのアクセスが実行され、操作の手間を省くことができる。また、ユーザは認証レベルを意識することなく操作することができ、分かり易いユーザ情報アクセス制御装置を実現できる。

【００４３】このように、実施形態のユーザ情報アクセス制御装置は、複数のユーザが端末を同時に使用している場合でも、ユーザ情報に設定されたユーザ条件と認証レベルとに基づいて、ユーザ情報を安全に保護しながら、ユーザ情報へのアクセスを実行する。

【００４４】なお、ユーザ識別手段に対する認証レベルの決定は、それぞれのユーザ識別手段で行ってもよいし、使用中ユーザ管理部113で決定してもよい。

【００４５】また、データアクセスタイプは、ユーザ情報管理部114で指定する場合について説明したが、アプリケーション100が指定してもよい。また、アプリケーションは、端末内で起動しているものに限らず、接続された他の端末機器上で動作するものでも構わない。

【００４６】また、個々のユーザ情報に対する認証レベル条件及びデータアクセスタイプは、ユーザ毎に設定してもよいし、すべてのユーザ情報に共通であってもよい。

【００４７】また、使用中ユーザ管理部113で使用中とされているユーザは、ユーザ識別手段からの通知あるいは使用中ユーザ管理部113内で設定された条件により使用中ユーザから除外されるが、より低い認証レベルが存在する場合は、除外する代わりに、認証レベルを下げてもよい。例えばリモコンボタンのボタンを押すのみの認証レベルが低いユーザ識別手段と、ＩＣカードを使った認証レベルの高いユーザ識別手段とが存在する場合に、ＩＣカードを使って認証し、その認証が無効となった時、使用中ユーザ管理部113では、使用中ユーザから削除してもよいし、認証レベルを下げてリモコン識別と同等に扱ってもよい。

【００４８】また、実施形態では、ユーザ情報に対応する認証レベル条件とデータアクセスタイプとを規定して、認証レベル条件及びユーザ条件に基づいてユーザ情報へのアクセスを制御する場合について説明したが、ユーザ条件のみに基づいてユーザ情報へのアクセスを制御することも可能である。その場合、例えば図２において、認証レベル条件203、205が記述されていないものをイメージすれば良い。

【００４９】また、認証レベル条件とユーザ条件とを判定する場合でも、それらの判定は、同時に行う必要はない。図２の例では、ユーザ情報中に認証レベルの条件を記述しているため、認証レベル条件とユーザ条件との判定が同時行われるが、アプリケーションの処理により認証レベルの判定を行うなどの場合は、ユーザ条件の可否→ユーザ情報アクセスを受けて、その後のアプリケーションの処理の段階で認証レベル条件の判定が行われる。このように、認証レベル条件とユーザ条件との判定は同時でなくても一向に構わない。

【００５０】また、本発明のユーザ情報アクセス制御装置は、ユーザが使用する端末の内部機能であっても、外部装置として端末に接続されるものであっても構わない。また、本発明のユーザ情報アクセス制御装置の機能は、ソフトウエアで実現しても、ハードウエアで実現しても構わない。

【００５１】また、本実施の形態では、ユーザ情報アクセス制御として、「データに対するアクセスの制御」の場合を説明しているが、その他にも「プログラムに対する実行の制御」など、ユーザ情報の範囲は様々な場合が有り得る。

【００５２】

【発明の効果】以上の説明から明らかなように、本発明のユーザ情報アクセス制御装置は、利用者が複数に及ぶ場合でも、ユーザ情報の保護を図りながら、ユーザ情報への効率的なアクセスが可能である。

【００５３】第二に、現在の使用中ユーザを常に画面上に表示することにより、ユーザは、自身が装置に認識されていることを知ることができ、また、画面上に表示が無い場合には、装置の認識を正常化する操作を行うことができる。その結果、ユーザが認識しないうちに不要なデータが書き込まれたり、また、必要なデータを保存し損なったりすることを防ぐことができる。

【００５４】第三に、複数人が同時に利用する状況の下で、順次操作ユーザが変わりユーザデータにアクセスするような場合でも、簡単な操作でアクセスユーザを変えることができる。

【００５５】第四に、複数人が同時に利用する状況の下で、順次操作ユーザが変わりユーザデータにアクセスするような場合でも、アクセスユーザを自動的に判断できるようになる。

【００５６】第五に、複数人が同時に利用する状況の下で、ユーザが自動的に判断できない場合でも、簡単な操作でアクセスユーザを選択することができる。

【００５７】第六に、ユーザ確認部を持つことで、現在のユーザ条件でアクセスするには危険なユーザ情報が含まれることをユーザに知らせ、ユーザが確認した上でユーザ情報へアクセスすることが可能になり、安全性を確保しながらスムーズにユーザ情報にアクセスすることができる。

【００５８】第七に、代替認証を行うことにより、通常端末操作を行わないユーザに対するユーザ情報にもアクセスし、サービスを提供することができる。

【００５９】第八に、認証の追完を可能にしているた

め、認証レベル条件が満たない場合でも、その場で必要なユーザ認証を行うことにより、操作の手間を省くことができる。また、ユーザは認証レベルを意識する必要がなく、分かり易いユーザ情報アクセス制御装置を提供することができる。

【図面の簡単な説明】

【図１】本発明の実施形態におけるユーザ情報アクセス制御装置の構成を示すブロック図、

【図２】実施形態の装置のユーザ情報管理部で管理されるユーザ情報を示す図、

【図３】実施形態の装置のユーザ情報アクセス制御部の制御を示す図、

【図４】実施形態の装置の使用中ユーザ管理部で管理されるユーザ管理情報を示す図、

【図５】実施形態の装置のユーザ選択部でユーザを選択する画面を示す図、

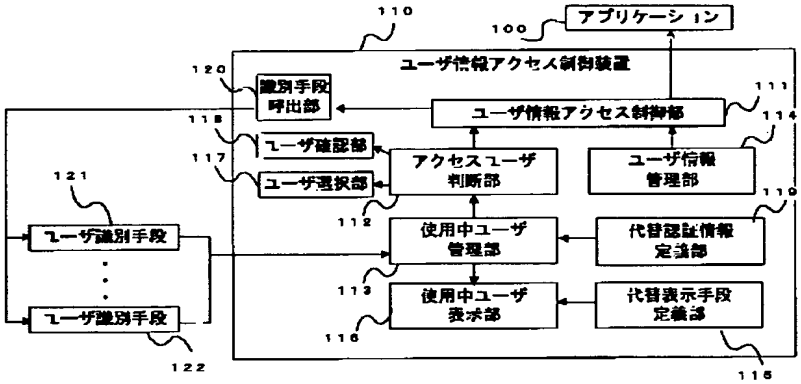
【図６】実施形態の装置の代替認証情報定義部で代替認証を行うための設定情報を示す図、

【図７】実施形態の装置の動作を示すフロー図である。

【符号の説明】

100　任意のアプリケーション
110　ユーザ情報アクセス制御装置
111　ユーザ情報アクセス制御部
112　アクセスユーザ判断部
113　使用中ユーザ管理部
114　ユーザ情報管理部
115　代替表示手段定義部
116　使用中ユーザ表示部
117　ユーザ選択部
118　ユーザ確認部
119　代替認証情報定義部
120　識別手段呼出部
121、122　任意のユーザ識別手段
201、211、221、231、241　ユーザ情報
202　ユーザ情報のデータ本体
203　読み込み認証レベル条件
204　読み込みデータアクセスタイプ
205　書き込み認証レベル条件
206　書き込みデータアクセスタイプ

【図１】



【図３】

データアクセスタイプ	ユーザ条件
SINGLE_W	1人
MULTI_W	1人以上
SINGLE_R	1人
MULTI_R	1人以上
USER_TYPE	同じユーザタイプのみ
ANY_ONE	複数人中一人自動選択
SELECT_ONE	複数人中ユーザ特定

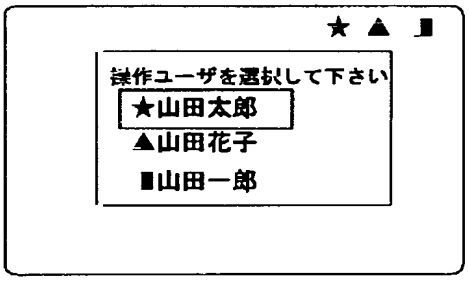
【図６】

認証済ユーザ		代替認証ユーザ	
ユーザID	認証レベル条件	ユーザID	認証レベル
1	2以上（数値2以下）	2	3
		3	3

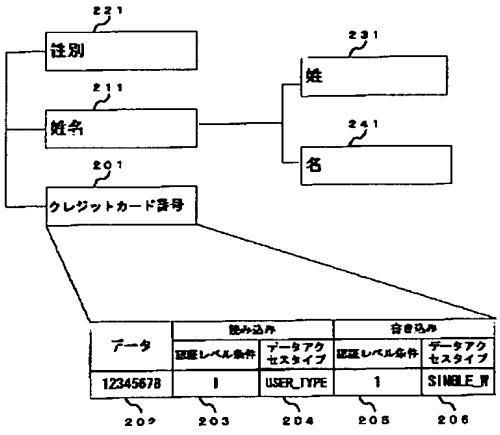
【図４】

ユーザID	認証レベル	識別時刻	入力デバイスID
1	3	15:30:21	remote-controller-1
3	3	15:30:21	remote-controller-2
4	1	16:00:05	keyboard-1

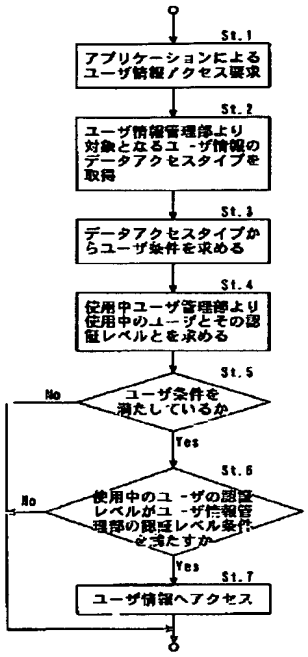
【図５】



【図2】



【図7】



フロントページの続き

Fターム(参考) 5B017 AA07 BA06 BB06 CA16
5B082 GA11
5B085 AA01 AA08 AE02 AE06
5C064 BA01 BA07 BB10 BC23 BC27
5J104 AA07 KA01 NA06 PA07